THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL DEFENDANT'S MOTION FOR EARLY RETURN OF TRIAL SUBPOENA TO CAPITAL ONE BANK (USA), N.A./CAPITAL ONE FINANCIAL CORP. **Noted: November 12, 2021**

Pursuant to Federal Rule of Criminal Procedure 17(c) and the Sixth Amendment, defendant Paige Thompson respectfully moves this Court to enter an order permitting the early return of a trial subpoena served on Capital One Bank (USA), N.A./Capital One Financial Corp. ("Capital One"). Capital One's documents are expected to play a critical evidentiary role in Ms. Thompson's defense. In support of the motion, Ms. Thompson submits the accompanying memorandum of law, and concurrently files an ex parte affidavit from counsel Mohammad Ali Hamoudi in camera and under seal and a proposed order calling for the return of the documents no later than 21 days after the date of the order.[1] The defense and Capital One have agreed that Capital One shall

[1] Ms. Thompson files the affidavit ex parte and in camera because it discusses and reveals defense strategy. *See* Fed. R. Crim. P. 17(b) (permitting "a defendant's ex parte

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

have 30 days to respond to this motion. The trial is currently scheduled for March 14, 2022.

DATED: October 4, 2021

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI

/s/ Christopher Sanders
CHRISTOPHER SANDERS

/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

/s/ Brian Klein
BRIAN KLEIN

/s/ Melissa Meister
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

---

application"). In *United States v. Sleugh*, 896 F.3d 1007, 1015 (9th Cir. 2018), the Ninth Circuit recognized the need to file affidavits in support of Rule 17(c) subpoenas under seal: "Such affidavits might sketch out possible defense theories," they "are not evidence themselves," and thus, "there is no presumption of public access under the First Amendment or common law that attaches to Rule 17(c) subpoena applications and their supporting materials." *See also United States v. Fry*, 2012 WL 117117, at *1 (E.D. Wa. Jan. 13, 2012) ("[T]he *ex parte* procedure is justified in circumstances where it is necessary to avoid disclosure of trial strategy or a witness list[.]"); *United States v. Tomison*, 969 F. Supp. 587 (E.D. Cal. 1997) (finding a Rule 17 ex parte submission appropriate to protect trial strategy).

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The superseding indictment paints a picture of Ms. Thompson as a "hacker" who illegally obtained unauthorized access to Capital One Bank (USA), N.A./Capital One Financial Corp.'s ("Capital One's") data located on Amazon Web Services ("AWS") servers for nefarious purposes, and then utilized that access to copy valuable financial information. The superseding indictment, however, fails to recognize that Ms. Thompson's alleged conduct with Capital One (and the other alleged victims) has a perfectly innocent explanation: It is the same type of conduct engaged in by so-called "white hat hackers," also known as computer security experts or "researchers," who patrol the Internet looking for vulnerabilities or "misconfigurations" in servers such as the one Ms. Thompson is alleged to have accessed.[2]

Proving criminal intent is paramount to this case, in which Ms. Thompson is charged with one count each of wire fraud, computer fraud and abuse, access device fraud, and aggravated identity theft as to Capital One. But the government has no credible evidence that Ms. Thompson attempted to monetize the allegedly valuable Capital One information (because she did not). This leaves the government grasping at two unrelated straws: (1) Ms. Thompson must have had criminal intent because after she allegedly accessed the AWS servers, she purportedly utilized their computing

[2] This motion focuses on the government's allegations with respect to Capital One's servers, which are found at Counts 1-2 and 8-10 of the superseding indictment. Counts 3-7 of the indictment relate to other entities and are not discussed in this motion.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

power to mine an insignificant amount of cryptocurrency; and/or (2) Ms. Thompson must have had criminal intent because she had in her possession personal identifying information (PII) that she could have monetized (though, again, there is no credible evidence that she actually did so).

Given the nature of the charges, Ms. Thompson has promulgated a series of subpoena requests to Capital One that are aimed directly at understanding Capital One's internal view of the alleged "misconfigurations" of the AWS servers and Ms. Thompson's access of them, as well as the alleged "value" of the information obtained and any monetary "loss" to Capital One due to Ms. Thompson's purported activities. These requests are directly relevant to whether Ms. Thompson had the specific intent to commit the crimes with which she as charged, and as such, are necessary for her defense in advance of trial. These are precisely the kinds of material that Federal Rule of Criminal Procedure 17(c) permits to be returned in advance of trial, and the Court should order such here so Ms. Thompson can adequately prepare her defense—including preparing at least one expert—in advance of trial.

II. RELEVANT FACTS

Ms. Thompson is charged in a ten-count superseding indictment. Counts 1-2 and 8-10 relate to Capital One and allege Ms. Thompson committed wire fraud in violation of 18 U.S.C § 1343 (Count 1); computer fraud and abuse in violation of 18 U.S.C. §§ 1030(a)(2)(A) and (C) and (c)(2)(A) and (B)(iii) (Count 2); computer fraud and abuse in violation of 18 U.S.C. §§ 1030(a)(5)(A) and (c)(4)(B)(i) (Count 8), access

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

device fraud (Count 9), and aggravated identity theft (Count 10).[3] (Dkt. No. 102; Aff. of Mohammad Ali Hamoudi ("Aff.") at ¶ 2.)

In general, regarding Capital One, the superseding indictment alleges Ms. Thompson "scanned" for "misconfigurations" in the "publicly facing portion" of cloud servers owned and operated by AWS, but rented by Capital One. (Docket No. 102.) According to the superseding indictment, once Ms. Thompson identified such misconfigurations, she "transmitted commands to the misconfigured servers that obtained the security credentials" belonging to Capital One. (*Id*.) Then after Ms. Thompson had these security credentials, it is alleged that she used them to obtain "lists or directories of folders or buckets of data," which she then copied to her own server; this data allegedly included "personal identifying information, from approximately 100,000,000 customers who had applied for credit cards from Capital One." (*Id*. at 4.) Additionally, the superseding indictment alleges that Ms. Thompson used the obtained security credentials to use the computing power of the AWS servers rented by Capital One to mine cryptocurrency, attempted to use PII taken from Capital One's servers to create unauthorized credit and debit cards, and intentionally and unlawfully possessed the PII of Capital One customers. (Id. at 5, 7-9.) The superseding indictment claims that the value of the information obtained by Ms. Thompson exceeded $5,000. (Id. at 6-8.)

[3] Counts 3-5 relate to three different entities and allege computer fraud and abuse in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(A) and (B)(iii). Counts 6-7 relate to two different entities and allege computer fraud and abuse in violation of 18 U.S.C. §§ 1030(a)(2)(C) and (c)(2)(A). (Dkt. No. 102; Aff. at ¶ 2.)

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

To sustain its burden of proof on the Capital One charges, the government must establish beyond a reasonable doubt, among other things, a scheme or artifice to defraud, Ms. Thompson's specific intent to defraud,[4] and that she intentionally accessed a computer without authorization or exceeding authorized access and thereby obtained financial and/or protected information. *See, e.g.*, *United States v. Jinian*, 725 F.3d 954, 960 (9th Cir. 2013) (wire fraud); *United States v. Manion*, 339 F.3d 1153, 1156 (9th Cir. 2003) (wire fraud); 18 U.S.C. §§ 1030(a)(2)(A) and (C) (CFAA); *United States v. Suphunthuchat,* 400 F. App'x 182, 183 (9th Cir. 2010) (access device fraud); *Flores-Figueroa v. United States*, 556 U.S. 646, 647 (2009) (aggravated identity theft). Because the government has also charged Ms. Thompson with a violation of 18 U.S.C. § 1030(c)(2)(B)(iii), it must also prove beyond a reasonable doubt that the value of the information Ms. Thompson allegedly obtained exceeded $5,000.

On May 4, 2020, pursuant to Rule 17(c), the defense issued a trial subpoena to Capital One that requested eleven categories of documents. (See 5/4/20 Subpoena and Attachment A, attached as Exhibit A.).[5] Once the subpoena was served on Capital One, counsel for both Capital One and Ms. Thompson met and conferred repeatedly via email, in writing, and telephonically on numerous occasions, and Capital One

---

[4] The government's burden is high, they must prove Ms. Thompson had a specific "intent to deceive and cheat." *United States v. Miller*, 953 F.3d 1095, 1103 (9th Cir. 2020), cert. denied, 141 S. Ct. 1085, 208 L. Ed. 2d 539 (2021) (emphasis added).

[5] The defense initially sent trial subpoenas to Capital One on October 10, 2019, but subsequently revised the subpoena requests. The ones attached to this motion are the most current version and the ones upon which the defense and Capital One has met and conferred since 2020.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

voluntarily produced documents and information responsive to the subpoena between July 27 and March 19, 2021. Between the date the subpoena was served and December 16, 2020, counsel were able to resolve eight of the eleven outstanding subpoena requests. However, as of the date of the filing of this motion, there remain three categories of documents in the subpoena that Capital One has either not produced or over which it has claimed a joint defense privilege with AWS.

The outstanding requests are:

Request No. 8

> Any communications involving anyone in the Company's Office of the Chief Information Security Officer or any Executive Officers (e.g., CEO, CFO, GC, and CIO) of the Company with anyone at Amazon Web Services relating to the Incident.

Request No. 10

> Any contracts between the Company and AWS relating to cloud infrastructure.

Request No. 11

> Any bills and invoices sent from AWS to the Company for providing cloud infrastructure from January 1, 2019 through December 31, 2020.

(Ex. A.) Before filing this motion, counsel for Ms. Thompson conferred telephonically with counsel for Capital One on April 13, 2021 regarding the bases for this motion and the remaining three subpoena requests. The parties were not able to agree as to the early return of any further subpoenaed materials from Capital One, thus necessitating the filing of this motion. Capital One has requested 30 days to oppose this motion. Ms. Thompson consents to that request and the noting date reflects that consent.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

III. ARGUMENT

The Court should order Capital One to produce documents responsive to Requests No. 8 and 10-11 (the "Requests") no later than 21 days after the Court's entry of order in this matter to ensure that Ms. Thompson has the materials sufficiently in advance of trial. The facts and circumstances of this case, as well as the law support such an order.

Given the nature of the Capital One charges, the alleged "misconfigurations" of the AWS servers rented by Capital One are central to Ms. Thompson's defense as those "misconfigurations" go directly to whether she accessed a computer without authorization or exceeding authorized access, as well as to her specific intent. The alleged "value" of the information obtained, as well as any monetary "loss" to Capital One due to Ms. Thompson's alleged exploitation of the "misconfigurations" is also directly relevant to the wire fraud and computer fraud and abuse charges.[6] These are precisely the kind of materials Rule 17(c) was intended to facilitate production of in advance of trial.

Rule 17 broadly allows defendants to subpoena third-party information and "is substantially the same as rule 45(a)" of the Civil Rules. See Fed. R. Crim. P. 17, adv. comm. n. 1944. While Rule 17 is not a discovery tool, in criminal cases, many district

[6] The documents sought are also highly relevant to sentencing, should Ms. Thompson proceed to that phase of the case. *See, e.g.,* USSG § 2B1.1(b)(1) (applying guidelines level increases for amount of loss); *id.* at (b)(10) (enhancement for "sophisticated means"); *id.* at (b)(11) (enhancement for use of an "authentication feature"); *id.* at (b)(17) (enhancement for "jeopardiz[ing] the safety and soundness of a financial institution"); *id.* at (b)(18) (enhancement for "intent to obtain personal information").

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

courts interpret the rule liberally. A liberal interpretation makes sense given the bizarre dichotomy between civil cases, where parties fighting over money have immense discovery powers, and criminal cases, where Ms. Thompson is fighting for her liberty has virtually no discovery powers: "It is ironic that a defendant in a breach of contract case" can "compel third-parties to produce any documents" that reasonably lead to discoverable evidence, while a "defendant on trial for his life or liberty does not even have the right to obtain documents 'material to his defense' from those same third-parties." *United States v. Nosal*, 291 F.R.D. 403, 408 (N.D. Cal. 2013) (quoting United *States v. Rajaratnam*, 753 F. Supp. 2d 317, 320 (S.D.N.Y. 2011) (citation omitted)); see *United States v. Tomison*, 969 F. Supp. 587, 593 n. 14 (E.D. Cal. 1997) (Rule 17(c) "may well be a proper device for discovering documents in the hands of third parties" and the full restrictions on Rule 17 "only apply to documents in the government's hands"); *Nixon,* 418 U.S. at 700 n.12 (reserving the issue of whether the restriction on discovery applies "in its full vigor when the subpoena duces tecum is issued to third parties rather than government prosecutors").

Rule17(c) authorizes courts to direct a party to produce materials designated in a subpoena before trial in order "to facilitate and expedite trials." *United States v. Carter*, 15 F.R.D. 367, 369 (D.D.C. 1954). Indeed, the "chief innovation" of Rule 17(c) was "to expedite the trial by providing a time and place before trial for the inspection of subpoenaed material." *United States v. Nixon*, 418 U.S. 683, 698-9 (1974) (citing *Bowman Dairy Co. v. United States,* 341 U.S. 214, 220 (1951)); see also *United States v. Gosar*, Nos. 19-306, 19-307-, 19-308, 19-313, 19-315, 19-320, 2020 WL 263613, at *1 (W.D. Wash. Jan. 17, 2020). To substantiate the early return of a trial subpoena, the

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

moving party must clear "three hurdles:" (1) relevancy; (2) admissibility; and (3) specificity. *Nixon,* 418 U.S. at 700; see *Gosar*, 2020 WL 263613, at *2.

Additionally, a court must consider whether the materials sought are "otherwise procurable reasonably in advance of trial by exercise of due diligence;" whether a defendant, like Ms. Thompson, can "properly prepare for trial without such production and inspection in advance of trial;" whether the "failure to obtain such inspection may tend unreasonably to delay the trial;" and whether the "application is made in good faith and is not intended as a general 'fishing expedition.'" *United States v. Krane*, 625 F.3d 568, 574 (9th Cir. 2010) (quoting *Nixon*, 418 U.S. at 699-700); see also *Gosar*, 2020 WL 263613, at *2. Ms. Thompson's request for the early return of materials from Capital One easily meets those requirements.

A. The Documents Sought From Capital One are Relevant, Admissible, and Described with the Requisite Particularity.

To establish relevancy, admissibility, and specificity, Ms. Thompson need only demonstrate a "sufficient likelihood," demonstrated through rational inferences that the documents sought "relate to the offenses charged in the indictment." *Pacific Gas*, 2016 WL 1212091, at *5; see *Nixon*, 418 U.S. at 700; *Bowman Dairy*, 341 U.S. at 219-20 (stating that it is sufficient if the subpoenaed material "could be used at trial"). The material requested in the Requests meets this standard.

The Requests are both specific and limited in temporal and categorical scope. Further, they are clearly relevant to the charges in the indictment. Ms. Thompson's "intent" is paramount to all of the charges levied against her by the government. The discovery produced to date indicates that Capital One initially referred to Ms.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

Thompson as a "researcher." It goes without saying that a person who accesses a firewall "misconfiguration" as a "researcher" has a far different intent than one who does so as a "hacker."

Ms. Thompson is entitled to discover through Capital One's communications with AWS (Request No. 8) how Capital One characterized Ms. Thompson's alleged actions and if (and when) that characterization changed. The contracts between Capital One and AWS relating to cloud infrastructure (Request No. 10) will help explain, exactly, what kind of cloud infrastructure Capital One was renting from AWS and will inform Ms. Thompson, potentially, about any limitations or configuration weaknesses AWS advised Capital One about from initiation of the relationship between the two parties. As for Request No. 11, the request for bills and invoices is directly relevant and admissible to the government's allegations of "cryptojacking" and concomitant damage to Capital One. The discovery sought by the Requests is not only relevant and admissible as to Ms. Thompson's defense of the government's charges, but it is also be relevant and admissible as impeachment evidence of any Capital One witnesses.

B. The Defense Requires the Requested Materials in Advance of Trial and Cannot Obtain the Material Through Other Means.

At present, there are no other means for Ms. Thompson to obtain the material requested but directly from Capital One—the materials requested are not in the government's discovery to date and are not in any way publicly accessible to Ms. Thompson.[7] The materials are also needed in advance of trial because they are

[7] Ms. Thompson has also issued third-party subpoenas to AWS and the Office of the Comptroller of the Currency ("OCC"). To date, AWS has not produced any documents pursuant to the subpoena, but arguably, AWS may also have documents relevant to

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

necessary for Ms. Thompson's expert(s) to review in preparation for her defense. If the materials were not provided in advance of trial, then it is likely that the trial would need to be delayed so that Ms. Thompson's defense team and experts could properly absorb the materials in the midst of trial. See *Nixon*, 418 U.S. at 702 (stating that a pre-trial return of materials is appropriate where the materials have "valid potential evidentiary uses" and analysis "may take a significant period of time"); *Pacific Gas*, 2016 WL 1212091, at *6 (noting that pre-trial return of "impeachment" materials is warranted when those same materials have other "valid potential evidentiary uses"). Thus, pretrial return of the materials requested from Capital One is appropriate and warranted.

C. The Subpoena is Neither Unreasonable Nor Oppressive.

Rule 17 subpoenas "may be quashed if their production would be 'unreasonable or oppressive,' but not otherwise." *Nixon*, 418 U.S. at 698. A Rule 17(c) subpoena, like this one, can be quashed as "unreasonable or oppressive" if it calls for privileged matter. See *Gosar*, 2020 WL 263613, at *2; *Pacific Gas*, 2016 WL 1212091, at *3. Here, the Requests are not unreasonable in their scope, which is appropriately and specifically limited both in time and in subject matter. Nonetheless, Capital One has invoked the "joint interest privilege" in withholding approximately eleven documents responsive to Request No. 8—communications between Capital One and AWS regarding Ms. Thompson's alleged exploitation of the "misconfigurations."

Request Nos. 8, 10, and 11. It is unknown whether the OCC is in possession of documents relevant to these same requests, although the defense is still engaged in the meet and confer process with the OCC.

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

The joint interest privilege, like any other testimonial privilege, is construed narrowly because it "contravenes the fundamental principal that the public has a right to every man's evidence" and it hinders the courts in the search for truth. *In re Pac. Pictures Corp*., 679 F.3d 1121, 1126 (9th Cir. 2012) (internal quotation marks and citation omitted); *see United States v. Bergonzi*, 216 F.R.D. 487, 497 (N.D. Cal. 2003). The joint interest privilege does not exist in isolation, but "presupposes the existence of an otherwise valid privilege" such as the attorney-client privilege or work product doctrine. *United States v. Omidi*, No. CR 17-661(A)-DMG, 2020 WL 6600172, at *1 (C.D. Cal. Aug. 12, 2020); *Waymo LLC v. Uber Techs., Inc.*, 319 F.R.D. 284, 292 (N.D. Cal. 2017). A "shared desire to see the same outcome in a legal matter is insufficient" to establish the joint interest privilege. *Omidi,* 2020 WL 6600172, at *1. Additionally, communications and/or documents prepared for the purpose of disclosing information to the government is not privileged. *See In re Syncor ERISA Litigation*, 229 F.R.D. 636, 645 (C.D. Cal. 2005). The party asserting the joint defense privilege has the "burden of establishing its existence," *Omidi*, 2020 WL 6600172, at *1, and "an assertion of privilege without evidence to support it will not prevail." *In re Syncor*, 229 F.R.D. at 644.

Capital One made its law enforcement referral on July 20, 2019. According to the privilege log produced by Capital One, Capital One and AWS had eleven allegedly privileged communications between July 22, 2019 and July 26, 2019, which is just a few days after Capital One's law enforcement referral and before Ms. Thompson was arrested on July 29, 2019. The privilege log is absolutely bereft of any information that explains why these communications are being withheld from Ms. Thompson other than

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

to say they involved "Capital One In-House Counsel's Legal Advice to the Company." Such explanation is insufficient to invoke the joint interest privilege here. To the extent that such documents are regarding communications with the government or in furtherance of a commercial interest in having a scapegoat for the alleged "misconfigurations," they are not privileged and must be produced.

IV. CONCLUSION

For the above stated reasons, Ms. Thompson respectfully requests that the Court grant this motion and order Capital One to produce the materials no later than 21 days after the Court's entry of the proposed order.

DATED: October 4, 2021.

Respectfully submitted,

/s/ Mohammad Ali Hamoudi
MOHAMMAD ALI HAMOUDI

/s/ Nancy Tenney
NANCY TENNEY
Assistant Federal Public Defenders

/s/ Christopher Sanders
CHRISTOPHER SANDERS

/s/ Brian Klein
BRIAN KLEIN

/s/ Melissa Meister
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100